3. YEAR IN REVIEW

On January 18, 2001, the Secretary of Energy directed that a review be conducted in response to the interim assessment of science and security at DOE laboratories by Dr. John Hamre, the Chair of the Congressional Commission on Science and Security. Subsequently, on January 19, 2001, Under Secretary Gordon issued a memorandum to the National Nuclear Security Administration (NNSA) wherein he directed a review of security policies and directives that had been issued over the past year and a "6-month hiatus from the implementation of new security requirements." The Office of Security and Emergency Operations concurred with this initiative, offered assistance in the conduct of the review, and is participating with NNSA, Defense Programs, and the Office of Science and Counterintelligence in the review. As part of this review, six working groups were established to review the various security policies and directives mentioned above. The working groups focused on the following areas: Foreign Visits and Assignments, Unclassified Nuclear Information, Tri-Lab 9/6 Measures, Enhancement Protective Measures, Unclassified Cyber Security Program, and Sensitive But Unclassified Information. An integrated report from the working groups summarized their findings and recommendations of the reviews.

Evidence of DOE's improved security efforts is found in a recently completed Congressionally mandated Red Team review of the Department's weapons laboratories' sensitive and classified systems and networks. The review showed that DOE had implemented a reasonable level of protection, and the Red Team was unable to penetrate any networks with classified or sensitive but unclassified information. Also, recent U.S. GAO and Office of Independent Oversight and Performance Assessment reviews have highlighted the positive changes that have taken place at many DOE sites. These reviews show that each DOE organization has focused on improving awareness of cyber security threats and implemented improved security controls.

The importance of information security can be seen in the recent restructuring by the newly appointed Secretary of Energy Spencer Abraham making the CIO position a direct report to the Office of the Secretary. This change to the management structure makes the CIO a full participant on the Department's executive management team and further defines the roles and responsibilities of the CIO.

The following is a summary of specific actions taken by DOE since the spring 2000 to improve the level of cyber security:

- Established cyber security policy and technical working groups to assist in formulating policy and guidance and providing technical advice to the CIO
- Provided $12.7 million for Cyber Security Architecture upgrades for various field offices
- Developed and piloted the Cyber Security Performance Measurement Program, which enables the evaluation of cyber security progress at the sites
- Issued a Departmentwide Cyber Security Architecture to provide a cyber security

framework for the operation of existing systems and the development of future systems

- Continued with the development and evaluation of site-specific CSPPs describing the implementation of cyber security protection at the sites
- Deployed Departmentwide training to improve the cyber security skills and knowledge of systems administrators, managers, and contractor personnel
- Continued to expand the PKI initiative, including publishing the PKI Strategy, Implementation Plan, Certificate Policy, and Architecture
- Cross-certified major laboratories for PKI
- Upgraded DOE site cyber security protection through the expanded use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerabilities.

DOE published a comprehensive Departmentwide cyber security management program, Order 205.1, that integrates not only risk management processes, but also physical, technical, and administrative controls for ensuring confidentiality, integrity, and availability of DOE's information assets. Under this program, a framework of objectives, guiding principles, and security activities and functions, which are applicable to classified and unclassified environments, are established to govern consistent implementation of cyber security management throughout the Department.

In summary, the current DOE Cyber Security Program bears little resemblance to the program set in place in the spring 1999. The Department has promulgated updated cyber security policies, improved the effectiveness of its security training for its system administrators, and informed management of upgraded cyber security threats. Each DOE site has a CSPP that identifies its security controls and planned upgrades. Finally, the Department has instituted a review and follow-up process using the Secretary's Independent Oversight function to permit an objective assessment of its status.